

**BEST AVAILABLE COPY**

PATENT  
81942.0013  
Express Mail Label No. EL 713 623 286 US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Yasuyuki MURAKAMI et al.

Serial No: Not assigned

Filed: January 23, 2001

For: SECRET KEY GENERATING METHOD,  
COMMON KEY GENERATING METHOD,  
ENCRYPTION METHOD, CRYPTOGRAPHIC  
COMMUNICATION METHOD AND  
CRYPTOGRAPHIC COMMUNICATION  
SYSTEM

Art Unit: Not assigned

Examiner: Not assigned



**TRANSMITTAL OF PRIORITY DOCUMENT**

Box PATENT APPLICATION  
Assistant Commissioner for Patents  
Washington, D.C. 20231

Dear Sir:

Enclosed herewith is a certified copy of Japanese patent application No. 2000-016354 which was filed January 25, 2000, from which priority is claimed under 35 U.S.C. § 119 and Rule 55.

Acknowledgment of the priority document(s) is respectfully requested to ensure that the subject information appears on the printed patent.

Respectfully submitted,

HOGAN & HARTSON L.L.P.

By: \_\_\_\_\_

Louis A. Mok  
Registration No. 22,585  
Attorney for Applicant(s)

Date: January 23, 2001

500 South Grand Avenue, Suite 1900  
Los Angeles, California 90071  
Telephone: 213-337-6700  
Facsimile: 213-337-6701

日本国特許庁  
PATENT OFFICE  
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日  
Date of Application: 2000年 1月25日

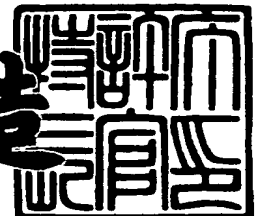
出願番号  
Application Number: 特願2000-016354

出願人  
Applicant(s): 村田機械株式会社  
笠原 正雄  
辻井 重男

2000年 8月18日

特許庁長官  
Commissioner,  
Patent Office

及川耕造



出証番号 出証特2000-3064840

【書類名】 特許願

【整理番号】 20871

【提出日】 平成12年 1月25日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00  
H04L 9/00

【発明の名称】 秘密鍵生成方法

【請求項の数】 3

【発明者】

【住所又は居所】 京都府京都市伏見区竹田向代町 1 3 6 番地 村田機械株式会社 本社工場内

【氏名】 村上 恭通

【発明者】

【住所又は居所】 大阪府箕面市栗生外院 4 丁目 1 5 番 3 号

【氏名】 笠原 正雄

【発明者】

【住所又は居所】 東京都渋谷区神宮前四丁目 2 番 1 9 号

【氏名】 辻井 重男

【特許出願人】

【識別番号】 000006297

【氏名又は名称】 村田機械株式会社

【代表者】 村田 純一

【特許出願人】

【識別番号】 597008636

【氏名又は名称】 笠原 正雄

【特許出願人】

【識別番号】 598159964

【氏名又は名称】 辻井 重男

【復代理人】

【識別番号】 100114557  
【弁理士】  
【氏名又は名称】 河野 英仁  
【電話番号】 06-6944-4141

【代理人】

【識別番号】 100078868  
【弁理士】  
【氏名又は名称】 河野 登夫  
【電話番号】 06-6944-4141

【手数料の表示】

【予納台帳番号】 001889  
【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1  
【物件名】 図面 1  
【物件名】 要約書 1  
【包括委任状番号】 9805283

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 秘密鍵生成方法

【特許請求の範囲】

【請求項 1】 複数のセンタの夫々にて、エンティティの特定情報を複数のブロックに分割した各分割特定情報と各センタ毎の秘密の対称行列とを用いて、前記エンティティ固有の秘密鍵を生成する方法において、前記各分割特定情報に応じて前記対称行列の一部の成分を取り出し、取り出した成分に前記エンティティ固有の乱数を合成することにより、前記エンティティ固有の秘密鍵を生成することを特徴とする秘密鍵生成方法。

【請求項 2】 一のセンタ自身で生成したハッシュ関数と他のセンタで生成されたハッシュ関数とに基づいて、前記一のセンタでの前記乱数を生成する請求項 1 に記載の秘密鍵生成方法。

【請求項 3】 複数のセンタの夫々にて、エンティティの特定情報を複数のブロックに分割した各分割特定情報と各センタ毎の秘密の対称行列とを用いて、前記エンティティ固有の秘密鍵を生成する方法において、前記各分割特定情報に応じて前記対称行列の一部の成分を取り出し、前記各分割特定情報に応じて各センタ固有のマスクパターンを生成し、取り出した成分を前記マスクパターンでマスクすることにより、前記エンティティ固有の秘密鍵を生成することを特徴とする秘密鍵生成方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、暗号通信システムのセンタにて各エンティティ固有の秘密鍵を生成する秘密鍵生成方法に関する。

【0002】

【従来の技術】

高度情報化社会と呼ばれる現代社会では、コンピュータネットワークを基盤として、ビジネス上の重要な文書・画像情報が電子的な情報という形で伝送通信されて処理される。このような電子情報は、容易に複写が可能である、複写物とオ

リジナルとの区別が困難であるという性質があり、情報保全の問題が重要視されている。特に、「コンピュータリソースの共有」，「マルチアクセス」，「広域化」の各要素を満たすコンピュータネットワークの実現が高度情報化社会の確立に不可欠であるが、これは当事者間の情報保全の問題とは矛盾する要素を含んでいる。このような矛盾を解消するための有効な手法として、人類の過去の歴史上主として軍事、外交面で用いられてきた暗号技術が注目されている。

## 【0003】

暗号とは、情報の意味が当事者以外には理解できないように情報を交換することである。暗号において、誰でも理解できる元の文（平文）を第三者には意味がわからない文（暗号文）に変換することが暗号化であり、また、暗号文を平文に戻すことが復号であり、この暗号化と復号との全過程をまとめて暗号系と呼ぶ。暗号化の過程及び復号の過程には、それぞれ暗号化鍵及び復号鍵と呼ばれる秘密の情報が用いられる。復号時には秘密の復号鍵が必要であるので、この復号鍵を知っている者のみが暗号文を復号でき、暗号化によって情報の秘密性が維持され得る。

## 【0004】

暗号化鍵と復号鍵とは、等しくても良いし、異なっても良い。両者の鍵が等しい暗号系は、共通鍵暗号系と呼ばれ、米国商務省標準局が採用したDES（Data Encryption Standards）はその典型例である。また、両者の鍵が異なる暗号系の一例として、公開鍵暗号系と呼ばれる暗号系が提案された。この公開鍵暗号系は、暗号系を利用する各ユーザ（エンティティ）が暗号化鍵と復号鍵とを一対ずつ作成し、暗号化鍵を公開鍵リストにて公開し、復号鍵のみを秘密に保持するという暗号系である。公開鍵暗号系では、この一対となる暗号化鍵と復号鍵とが異なり、一方向性関数を利用することによって暗号化鍵から復号鍵を割り出せないという特徴を持たせている。

## 【0005】

公開鍵暗号系は、暗号化鍵を公開するという画期的な暗号系であって、高度情報化社会の確立に必要な上述した3つの要素に適合するものであり、情報通信技術の分野等での利用を図るべく、その研究が活発に行われ、典型的な公開鍵暗号

系としてRSA暗号系が提案された。このRSA暗号系は、一方向性関数として素因数分解の困難さを利用して実現されている。また、離散対数問題を解くことの困難さ（離散対数問題）を利用した公開鍵暗号系も種々の手法が提案されてきた。

## 【0006】

また、各エンティティの住所、氏名等の個人を特定するID (Identity) 情報を利用する暗号系が提案された。この暗号系では、ID情報に基づいて送受信者間で共通の暗号化鍵を生成する。また、このID情報に基づく暗号技法には、(1) 暗号文通信に先立って送受信者間での予備通信を必要とする方式と、(2) 暗号文通信に先立って送受信者間での予備通信を必要としない方式とがある。特に、(2)の手法は予備通信が不要であるので、エンティティの利便性が高く、将来の暗号系の中樞をなすものと考えられている。

## 【0007】

この(2)の手法による暗号系は、ID-NIKS (ID-based non-interactive key sharing scheme)と呼ばれており、通信相手のID情報を用いて予備通信を行うことなく暗号化鍵を共有する方式を採用している。ID-NIKSは、送受信者間で公開鍵、秘密鍵を交換する必要がなく、また鍵のリスト及び第三者によるサービスも必要としない方式であり、任意のエンティティ間で安全に通信を行える。

## 【0008】

図5は、このID-NIKSのシステムの原理を示す図である。信頼できるセンタの存在を仮定し、このセンタを中心にして共通鍵生成システムを構成している。図5において、エンティティXの特定情報であるエンティティXの名前、住所、電話番号等のID情報は、ハッシュ関数 $h(\cdot)$ を用いて $h(ID_X)$ で表す。センタは任意のエンティティXに対して、センタ公開情報 $\{PC_i\}$ 、センタ秘密情報 $\{SC_i\}$ 及びエンティティXのID情報 $h(ID_X)$ に基づいて、以下のように秘密情報 $S_{Xi}$ を計算し、秘密裏にエンティティXへ配布する。

$$S_{Xi} = F_i(\{SC_i\}, \{PC_i\}, h(ID_X))$$

## 【0009】

エンティティ X は他の任意のエンティティ Y との間で、暗号化、復号のための共通鍵  $K_{XY}$  を、エンティティ X 自身の秘密情報  $\{S_{Xi}\}$ 、センタ公開情報  $\{PC_i\}$  及び相手先のエンティティ Y の ID 情報  $h(ID_Y)$  を用いて以下のように生成する。

$$K_{XY} = f(\{S_{Xi}\}, \{PC_i\}, h(ID_Y))$$

また、エンティティ Y も同様にエンティティ X への鍵を共通鍵  $K_{YX}$  を生成する。もし常に  $K_{XY} = K_{YX}$  の関係が成立すれば、この鍵  $K_{XY}$ 、 $K_{YX}$  をエンティティ X、Y 間で暗号化鍵、復号鍵として使用できる。

#### 【0010】

上述した公開鍵暗号系では、例えば RSA 暗号系の場合にその公開鍵の長さは現在の電話番号の十数倍となり、極めて煩雑である。これに対して、ID-NIKS では、各 ID 情報を名簿という形式で登録しておけば、この名簿を参照して任意のエンティティとの間で共通鍵を生成することができる。従って、図 5 に示すような ID-NIKS のシステムが安全に実現されれば、多数のエンティティが加入するコンピュータネットワーク上で便利な暗号系を構築できる。このような理由により、ID-NIKS が将来の暗号系の中心になると期待されている。

#### 【0011】

この ID-NIKS には、次のような 2 つの問題点がある。一つは、センタが Big Brother となる（すべてのエンティティの秘密を握っており、Key Escrow System になってしまう）点である。もう一つは、ある数のエンティティが結託するとセンタの秘密を演算できる可能性がある点である。この結託問題については、これを計算量的に回避するための工夫が多数なされているが、完全な解決は困難である。

#### 【0012】

この結託問題の難しさは、特定情報（ID 情報）に基づく秘密パラメータがセンタ秘密と個人秘密との二重構造になっていることに起因する。ID-NIKS では、センタの公開パラメータと個人の公開された特定情報（ID 情報）とこの 2 種類の秘密パラメータとにて暗号系が構成され、しかも各エンティティが各自に配布された個人秘密を見せ合ってもセンタ秘密が露呈されないようにする必要



がある。よって、その暗号系の構築の実現には解決すべき課題が多い。

【0013】

そこで、本発明者等は、特定情報（ID情報）をいくつかに分割し、複数のセンタの夫々からその分割した特定情報（ID情報）に基づくすべての秘密鍵をエンティティに配布することにより、数学的構造を最小限に抑えることができ、結託問題の回避を可能にし、その暗号系の構築が容易であるID-NIKSによる暗号手法（以下、これを先行例という）を提案している。

【0014】

結託問題を解決することを目的として提案されてきたエンティティの特定情報（ID情報）に基づく種々の暗号系が不成功となった理由は、エンティティの結託情報からセンタ秘密を割り出せないようにするための工夫を数学的構造に求め過ぎていたためである。数学的構造が複雑過ぎると、安全性を証明するための方法も困難となる。そこで、先行例の提案方法では、エンティティの特定情報（ID情報）をいくつかに分割し、分割した各特定情報（ID情報）についてすべての秘密鍵をエンティティに配布することにより、数学的構造を最小限に抑えるようにする。

【0015】

先行例では、信頼される複数のセンタが設けられ、各センタは各エンティティの分割した各特定情報（ID情報）に対応する数学的構造を持たない秘密鍵を夫々生成して、各エンティティへ送付する。各エンティティは、各センタから送られてきたこれらの秘密鍵と通信相手の公開されている特定情報（ID情報）とから共通鍵を、予備通信を行わずに生成する。これらの各秘密鍵に含まれている通信相手に対応する成分を夫々取り出し、取り出した成分を合成加算して共通鍵を生成する。よって、すべてのエンティティの秘密を1つのセンタが握るようなことはなく、各センタがBig Brotherにならない。

【0016】

以下、この先行例の概要を説明する。各エンティティの氏名、住所などを示す特定情報であるIDベクトルをL次元2進ベクトルとし、そのIDベクトルをブロックサイズM毎にJ個のブロックに分割する。例えば、エンティティXのID

ベクトル (ベクトル  $I_X$ ) を下記 (1) のように分割する。分割特定情報である各ベクトル  $I_{Xj}$  ( $j = 1, 2, \dots, J$ ) を ID 分割ベクトルと呼ぶ。なお、各エンティティの公開 ID ベクトルはハッシュ関数により、 $L (=MJ)$  ビットに変換される。また、ID ベクトルの分割数に応じて  $J$  個のセンタを設置し、 $j = 1, 2, \dots, J$  をセンタ番号とする。

【0017】

【数1】

$$\overrightarrow{I_X} = [\overrightarrow{I_{X1}} \mid \overrightarrow{I_{X2}} \mid \dots \mid \overrightarrow{I_{XJ}}] \quad \dots (1)$$

【0018】

$j$  番目のセンタは、ランダムな数を要素とする対称行列  $H_j$  ( $2^M \times 2^M$ ) を作成する。但し、共通鍵のサイズを  $S$  として、下記 (2) ~ (4) とする。

【0019】

【数2】

$$H_j = (k_{ab}^{(j)}) \quad \dots (2)$$

$$k_{ab}^{(j)} \in Z_{2^S} \quad \dots (3)$$

$$a, b \in Z_{2^M} \quad \dots (4)$$

【0020】

また、 $j$  番目のセンタは、各エンティティに対して、対称行列  $H_j$  より、そのエンティティの ID 分割ベクトルに対応する行ベクトルを秘密配布する。即ち、エンティティ  $X$  に対しては、ベクトル  $s_{Xj} = H_j$  [ベクトル  $I_{Xj}$ ] を配布する。この  $H_j$  [ベクトル  $I_{Xj}$ ] は、対称行列  $H_j$  よりベクトル  $I_{Xj}$  に対応した行を 1 行抜き出したベクトルを表す。各エンティティに配布されたパラメータを秘密ベクトルと呼ぶ。

【0021】

エンティティ  $X$ ,  $Y$  間で共通鍵を共有するとする。エンティティ  $X$  は、各セン

タから受け取った各秘密ベクトルから、エンティティ Y に対応する成分を取り出し、これらの J 個の成分を合成することにより、エンティティ Y に対する共通鍵を生成する。エンティティ Y も、エンティティ X に対する共通鍵を同様に生成する。各センタで生成する秘密行列  $H_j$  の対称性によって、エンティティ X, Y は同一の共通鍵を共有できる。このようにして生成した共通鍵を用いて、エンティティ X, Y 間での暗号化処理・復号処理を行う。

## 【 0 0 2 2 】

## 【発明が解決しようとする課題】

本発明者等は、このような先行例の改良を研究しており、その先行例を適用した暗号通信システムの構築を図っている。この先行例は、非常に高速に共通鍵を共有できるという優れた長所を有する。しかしながら、各エンティティにとって、全体の ID ベクトルが一致することは考えられないが、その一部である ID 分割ベクトルが同一となることは考えられる。よって、複数のエンティティが結託して、自身の秘密の部分鍵を提供することにより、各エンティティの ID 分割ベクトルの合成にてその全体の ID ベクトルが構成される他のエンティティになりすますという結託攻撃に弱いという難点があり、更なる改善が望まれている。このような難点は、各センタの秘密の対称行列の一部をそのままエンティティへ配布していることに起因する。

## 【 0 0 2 3 】

本発明は斯かる事情に鑑みてなされたものであり、先行例と同様に鍵共有の高速性は維持しながら、先行例と比べて安全性を向上できる秘密鍵生成方法を提供することを目的とする。

## 【 0 0 2 4 】

## 【課題を解決するための手段】

請求項 1 に係る秘密鍵生成方法は、複数のセンタの夫々にて、エンティティの特定情報を複数のブロックに分割した各分割特定情報と各センタ毎の秘密の対称行列とを用いて、前記エンティティ固有の秘密鍵を生成する方法において、前記各分割特定情報に応じて前記対称行列の一部の成分を取り出し、取り出した成分に前記エンティティ固有の乱数を合成することにより、前記エンティティ固有の

秘密鍵を生成することを特徴とする。

【0025】

請求項2に係る秘密鍵生成方法は、請求項1において、一のセンタ自身で生成したハッシュ関数と他のセンタで生成されたハッシュ関数とに基づいて、前記一のセンタでの前記乱数を生成することを特徴とする。

【0026】

請求項3に係る秘密鍵生成方法は、複数のセンタの夫々にて、エンティティの特定情報を複数のブロックに分割した各分割特定情報と各センタ毎の秘密の対称行列とを用いて、前記エンティティ固有の秘密鍵を生成する方法において、前記各分割特定情報に応じて前記対称行列の一部の成分を取り出し、前記各分割特定情報に応じて各センタ固有のマスクパターンを生成し、取り出した成分を前記マスクパターンでマスクすることにより、前記エンティティ固有の秘密鍵を生成することを特徴とする。

【0027】

第1発明では、エンティティの各分割特定情報（ID分割ベクトル）に応じて対称行列の一部の成分を取り出し、取り出した成分に各エンティティ固有の乱数を合成して、各エンティティ固有の秘密鍵を生成する。よって、個人乱数を加えるので、センタの秘密が露呈されず、安全性が向上する。

【0028】

第2発明では、第1発明において、自身で生成したハッシュ関数と他のセンタで生成されたハッシュ関数とを用いて、取り出した成分に合成すべき乱数を生成する。よって、全てのセンタが対等となり、ある特定のセンタがBig Brother なることを防止できる。

【0029】

第3発明では、エンティティの各分割特定情報（ID分割ベクトル）に応じて対称行列の一部の成分を取り出し、その分割特定情報（ID分割ベクトル）に基づいて各センタ固有のマスクパターンを生成し、取り出した成分をそのマスクパターンでマスクして、各エンティティ固有の秘密鍵を生成する。よって、両エンティティにおいて分割特定情報（ID分割ベクトル）が同じであっても、そのマ

スクパターンは異なり、結託攻撃に強くなる。

【0030】

第1発明及び第3発明の特徴を併せた手法にて各エンティティ固有の秘密鍵を生成する場合には、乱数置換攻撃が成立しない。

【0031】

また、本発明では、共通鍵を生成する際に各センタからの成分をXOR合成しており、桁上がりの問題を解消している。

【0032】

【発明の実施の形態】

以下、本発明の実施の形態について具体的に説明する。

図1は、本発明の暗号通信システムの構成を示す模式図である。情報の隠匿を信頼できる複数（J個）のセンタ1が設定されており、これらのセンタ1としては、例えば社会の公的機関を該当できる。

【0033】

これらの各センタ1と、この暗号通信システムを利用するユーザとしての複数の各エンティティa, b, ..., zとは、通信路 $2_{a1}$ , ...,  $2_{aJ}$ ,  $2_{b1}$ , ...,  $2_{bJ}$ , ...,  $2_{z1}$ , ...,  $2_{zJ}$ により接続されており、これらの通信路を介して、各センタ1から各エンティティ固有の秘密鍵（秘密ベクトル）が各エンティティa, b, ..., zへ伝送されるようになっている。また、2人のエンティティの間には通信路 $3_{ab}$ ,  $3_{az}$ ,  $3_{bz}$ , ...が設けられており、この通信路 $3_{ab}$ ,  $3_{az}$ ,  $3_{bz}$ , ...を介して通信情報を暗号化した暗号文が互いのエンティティ間で伝送されるようになっている。

【0034】

図2は、2人のエンティティa, b間における情報の通信状態を示す模式図である。図2の例は、エンティティaが平文（メッセージ）Mを暗号文Cに暗号化してそれをエンティティbへ送信し、エンティティbがその暗号文Cを元の平文（メッセージ）Mに復号する場合を示している。

【0035】

j（j = 1, 2, ..., J）番目のセンタ1には、各エンティティのa, b

の分割特定情報（分割IDベクトル）を用いて各エンティティ a, b 固有の秘密鍵を生成する秘密鍵生成器 1a が備えられている。そして、各エンティティ a, b から登録が依頼されると、そのエンティティ a, b の秘密鍵（秘密ベクトル）がエンティティ a, b へ送付される。

## 【0036】

エンティティ a 側には、J 個の各センタ 1 から送られる固有の秘密鍵をテーブル形式で格納しているメモリ 10 と、これらの秘密鍵の中からエンティティ b に対応する成分を選び出す成分選出器 11 と、選び出されたこれらの成分を合成してエンティティ a が求めるエンティティ b との共通鍵  $K_{ab}$  を生成する共通鍵生成器 12 と、共通鍵  $K_{ab}$  を用いて平文（メッセージ）M を暗号文 C に暗号化して通信路 30 へ出力する暗号化器 13 とが備えられている。

## 【0037】

また、エンティティ b 側には、各センタ 1 から送られる固有の秘密鍵をテーブル形式で格納しているメモリ 20 と、これらの秘密鍵の中からエンティティ a に対応する成分を選び出す成分選出器 21 と、選び出されたこれらの成分を合成してエンティティ b が求めるエンティティ a との共通鍵  $K_{ba}$  を生成する共通鍵生成器 22 と、共通鍵  $K_{ba}$  を用いて通信路 30 から入力した暗号文 C を平文（メッセージ）M に復号して出力する復号器 23 とが備えられている。

## 【0038】

次に、このような構成の暗号通信システムにおける暗号通信の処理動作について説明する。

## 【0039】

## （予備処理）

各エンティティの氏名、住所などを示す特定情報である ID ベクトルを L 次元 2 進ベクトルとし、図 3 に示すようにその ID ベクトルをブロックサイズ  $M_1$ ,  $M_2$ ,  $\dots$ ,  $M_J$  毎に J 個のブロックに分割する。例えば、エンティティ a の ID ベクトル（ベクトル  $I_a$ ）を下記（5）のように分割する。分割特定情報である各ベクトル  $I_{aj}$  ( $j = 1, 2, \dots, J$ ) を ID 分割ベクトルと呼ぶ。ここで、 $M_j = M$  とすると、全ての ID 分割ベクトルのサイズが等しくなる。また

、 $M_j = 1$ と設定することも可能である。なお、各エンティティの公開IDベクトルはハッシュ関数により、 $L$ ビットに変換される。なお、以下では説明を簡単にするために、 $M_j = M$ （一定）とする。

【0040】

【数3】

$$\vec{I}_a = [ \vec{I}_{a1} \mid \vec{I}_{a2} \mid \cdots \mid \vec{I}_{aJ} ] \quad \cdots (5)$$

【0041】

以下、本発明の3種の例について具体的に説明する。

（第1実施の形態）

〔秘密鍵の生成・配布処理〕

$j$  番目のセンタ1は、ランダムな数を要素とする対称行列 $H_j$  ( $2^M \times 2^M$ ) を生成する。但し、共通鍵のサイズを $S$ として、上記(2)～(4)の条件を満たす。

【0042】

また、 $j$  番目のセンタ1は、 $S$ ビットを出力するハッシュ関数 $f_j(\cdot)$  を生成し、秘密裏に次の $(j+1)$  番目のセンタ1へ送付する。但し、 $J$  番目のセンタ1は、1 番目のセンタ1へ送付する。

【0043】

そして、 $j$  番目のセンタ1は、エンティティ $a$ に対して、対称行列 $H_j$  より、そのエンティティ $a$ のID分割ベクトルに対応する行ベクトルを取り出し、取り出した行ベクトルの全ての成分に個人乱数 $\alpha_a^{(j)}$  をXORしたものを秘密鍵ベクトル $s_{aj}$ として生成し、それをエンティティ $a$ へ秘密裏に配布する。

【0044】

即ち、 $m=0, 1, 2, \dots, 2^M - 1$  に対して、下記(6)を秘密鍵ベクトル $s_{aj}$ として配布する。なお、 $\alpha_a^{(j)}$  を、下記(7)のように設定する。但し、 $j-1=0$ である場合には $J$ として扱う。なお、 $k_{aj,m}^{(j)}$  は、エンティティ $a$ のID分割ベクトルに対応する行ベクトルの各成分を示す。

【0045】

【数4】

$$s_{a_j, m} = k_{a_j, m}^{(j)} \oplus \alpha_a^{(j)} \quad \dots (6)$$

$$\alpha_a^{(j)} = f_j(ID_a) \oplus f_{j-1}(ID_a) \quad \dots (7)$$

【0046】

〔共通鍵の生成（鍵共有）〕

エンティティ a は、J 個の各センタから受け取った秘密ベクトルから、エンティティ b に対応する成分を取り出し、これらの J 個の成分を XOR により合成して、エンティティ b に対する共通鍵  $K_{ab}$  を生成する。この際、エンティティ a に関する全ての個人乱数  $\alpha_a^{(j)}$  を XOR した場合、同一のハッシュ値が 2 度ずつ XOR されて 0 になるので、下記 (8) が成立する。

【0047】

【数5】

$$\begin{aligned} K_{ab} &= \bigoplus_{j=1}^J s_{a_j, b_j} \\ &= \bigoplus_{j=1}^J \left( k_{a_j, b_j}^{(j)} \oplus \alpha_a^{(j)} \right) \\ &= \bigoplus_{j=1}^J k_{a_j, b_j}^{(j)} \quad \dots (8) \end{aligned}$$

【0048】

エンティティ b も、エンティティ a に対して共通鍵  $K_{ba}$  を同様に生成する。ここで、J 個の各センタ 1 が有する秘密情報（行列  $H_j$ ）の対称性に基づいて、両



共通鍵  $K_{ab}$ ,  $K_{ba}$  は一致する。

【 0 0 4 9 】

この第 1 実施の形態では、センタの秘密が露呈しないので、安全性が高い。また、各エンティティの個人乱数を設定するような特定のセンタの存在は不要であり、Big Brother の問題を全く排除している。

【 0 0 5 0 】

(第 2 実施の形態)

〔秘密鍵の生成・配布処理〕

$j$  番目のセンタ 1 は、第 1 実施の形態と同様に、対称行列  $H_j$  を生成する。また、 $S$  ビットを出力する関数  $g_j(\cdot)$  を生成して公開する。

【 0 0 5 1 】

そして、 $j$  番目のセンタ 1 は、エンティティ  $a$  について、対称行列  $H_j$  より、そのエンティティ  $a$  の ID 分割ベクトルに対応する行ベクトルを取り出し、取り出した行ベクトルの全ての成分に対して、 $g_j(ID_a)$  のビットパターンによりマスクしたものを秘密鍵ベクトル  $s_{aj}$  として生成し、それをエンティティ  $a$  へ秘密裏に配布する。なお、ここでのマスク処理は、ビット毎の AND 演算である。

【 0 0 5 2 】

〔共通鍵の生成（鍵共有）〕

エンティティ  $a$  は、 $J$  個の各センタから受け取った秘密ベクトルから、エンティティ  $b$  に対応する成分を取り出し、これらの成分に対して  $g_j(ID_b)$  を自身の秘密鍵の各成分にマスクした値を、 $j = 1$  から  $J$  まで XOR により合成して、エンティティ  $b$  に対する共通鍵  $K_{ab}$  を生成する。即ち、下記 (9) が成立する。

【 0 0 5 3 】

【数 6】

$$\begin{aligned}
 K_{ab} &= \bigoplus_{j=1}^J (s_{a_j b_j} \cap g_j(ID_b)) \\
 &= \bigoplus_{j=1}^J k_{a_j b_j}^{(j)} \cap g_j(ID_a) \cap g_j(ID_b) \\
 &\dots (9)
 \end{aligned}$$

【0054】

エンティティ b も、エンティティ a に対して共通鍵  $K_{ba}$  を同様に生成する。ここで、J 個の各センタ 1 が有する秘密情報（行列  $H_j$ ）の対称性に基づいて、両共通鍵  $K_{ab}$ 、 $K_{ba}$  は一致する。

【0055】

この第 2 実施の形態では、配布される秘密鍵には、センタが生成した秘密情報（行列  $H_j$ ）のうちの一部の情報しか含まれていない。例えば、エンティティ a、b の ID ベクトルが部分的に等しい場合でも、マスク  $g_j(ID_a)$  と  $g_j(ID_b)$  とが異なるので、秘密鍵ベクトル  $s_{a_j}$  と  $s_{b_j}$  とは同一でない。従って、センタの秘密行列の全情報を得るためには、非常に多数のエンティティによる結託が必要であり、結託閾値を高くすることができる。

【0056】

（第 3 実施の形態）

上述した第 1 実施の形態、第 2 実施の形態を融合した第 3 実施の形態について説明する。この第 3 実施の形態は、乱数置換攻撃が成立しないという特徴を有する。

【0057】

〔秘密鍵の生成・配布処理〕

j 番目のセンタ 1 は、第 1 実施の形態と同様に、対称行列  $H_j$  を生成する。また、j 番目のセンタ 1 は、S ビットを出力するハッシュ関数  $f_j(\cdot)$  を生成し

、秘密裏に次の  $(j+1)$  番目のセンタ 1 へ送付する。但し、 $J$  番目のセンタ 1 は、1 番目のセンタ 1 へ送付する。また、 $S$  ビットを出力する関数  $g_j(\cdot)$  を生成して公開する。

【0058】

そして、 $j$  番目のセンタ 1 は、エンティティ  $a$  について、対称行列  $H_j$  より、そのエンティティ  $a$  の ID 分割ベクトルに対応する行ベクトルを取り出し、取り出した行ベクトルの全ての成分に対して、 $g_j(ID_a)$  のビットパターンによりマスクし、更に個人乱数  $\alpha_a^{(j)}$  を XOR したものを秘密鍵ベクトル  $s_{aj}$  として生成し、それをエンティティ  $a$  へ秘密裏に配布する。なお、ここでのマスク処理は、ビット毎の AND 演算である。

【0059】

即ち、 $m=0, 1, 2, \dots, 2^M-1$  に対して、下記 (10) を秘密鍵ベクトル  $s_{aj}$  として配布する。なお、 $\alpha_a^{(j)}$ ,  $\beta_a^{(j)}$  を、下記 (11), (12) のように設定する。但し、 $j-1=0$  である場合には  $J$  として扱う。

【0060】

【数 7】

$$s_{aj,m} = \left( k_{a,j,m}^{(j)} \cap \beta_a^{(j)} \right) \oplus \alpha_a^{(j)} \quad \dots (10)$$

$$\alpha_a^{(j)} = f_j(ID_a) \oplus f_{j-1}(ID_a) \quad \dots (11)$$

$$\beta_a^{(j)} = g_j(ID_a) \quad \dots (12)$$

【0061】

〔共通鍵の生成（鍵共有）〕

エンティティ  $a$  は、 $J$  個の各センタから受け取った秘密ベクトルから、エンティティ  $b$  に対応する成分を取り出し、第 1 実施の形態と同様に、これらの  $J$  個の成分を XOR により合成して、下記 (13) のように中間鍵  $K_{ab}'$  を生成する。こ

の際、エンティティ a に関する同一のハッシュ値が 2 度ずつ XOR されて 0 になることは、第 1 実施の形態と同様である。

【0062】

【数 8】

$$K_{ab'} = \bigoplus_{j=1}^J s_{a_j} b_j \quad \dots (13)$$

【0063】

次に、中間鍵  $K_{ab'}$  から、互いのマスク値を考慮して、有効なビット成分を抜き出して、下記 (14) のように、エンティティ b に対する共通鍵  $K_{ab}$  を生成する。但し、バー x は x のビット毎の否定演算を表す。

【0064】

【数 9】

$$K_{ab} = K_{ab'} \cap \bigcap_{j=1}^J \overline{\beta_a^{(j)} \oplus \beta_b^{(j)}} \quad \dots (14)$$

【0065】

エンティティ b も、エンティティ a に対して共通鍵  $K_{ba}$  を同様に生成する。ここで、J 個の各センタ 1 が有する秘密情報（行列  $H_j$ ）の対称性に基づいて、両共通鍵  $K_{ab}$ 、 $K_{ba}$  は一致する。

【0066】

この第 3 実施の形態における安全性について説明する。第 3 実施の形態では、各ブロックに個人乱数が XOR されているので、第 2 実施の形態のようにブロック毎にセンタの秘密行列の部分情報が漏れることはない。また、特定のエンティティを攻撃するために乱数置換攻撃を適用した場合であっても、マスク処理の影

響によって、この攻撃は成立しない。

【 0 0 6 7 】

第 3 実施の形態では第 2 実施の形態と同様、結託閾値を向上させるためにマスク処理という手法を用いている。よって、安全性は向上するが、 $J$  を大きくした場合、最終的に鍵共有に使用可能な有効ビットの数が急激に減少することが考えられる。そこで、このことを解消するために、次の (a) , (b) のような対策が可能である。

【 0 0 6 8 】

(a) 暗号通信システム全体で共通の関数  $g(\cdot)$  を設定し、各センタが設定しているマスク値を求める関数を  $g_j(\cdot) = g(\cdot)$  とする。

(b) 暗号通信システム全体で共通の関数  $g(\cdot)$  を設定し、前半  $J/2$  のセンタは  $g_j(\cdot) = g(\cdot)$  とし、後半  $J/2$  のセンタは  $g_j(\cdot) = \text{バー } g(\cdot)$  とする。

【 0 0 6 9 】

(a) の対策では、マスク部分が減少するようなことはないが、0 でマスクされていた部分は鍵共有時に 0 となるので、関数  $g(\cdot)$  が 0 と 1 とを一様に出力すると仮定した場合、鍵共有に使用される有効部分は全体の  $1/4$  程度となる。

【 0 0 7 0 】

(b) の対策では、下記 (15) が成立するので、上記 (14) のマスク部分が減少することはない。しかしながら前半のセンタにおいて 0 でマスクされていたために鍵共有時に 0 となる部分が、後半のセンタにおいては 1 でマスクされているために鍵共有時に有効となる。このため、関数  $g(\cdot)$  が 0 と 1 とを一様に出力すると仮定した場合、鍵共有に使用される有効部分は全体の  $1/2$  程度となる。

【 0 0 7 1 】

【数 10】

$$g(ID_a) \oplus g(ID_b) = \overline{g(ID_a) \oplus g(ID_b)}$$

... (15)

【0072】

図4は、本発明の記録媒体の実施の形態の構成を示す図である。ここに例示するプログラムは、上述した第1実施の形態における各エンティティ固有の秘密鍵の生成処理、第2実施の形態における各エンティティ固有の秘密鍵の生成処理または第3実施の形態における各エンティティ固有の秘密鍵の生成処理を含んでおり、以下に説明する記録媒体に記録されている。なお、コンピュータ40は、各センタ側に設けられている。

【0073】

図4において、コンピュータ40とオンライン接続する記録媒体41は、コンピュータ40の設置場所から隔たって設置される例えばWWW(World Wide Web)のサーバコンピュータを用いてなり、記録媒体41には前述の如きプログラム41aが記録されている。記録媒体41から読み出されたプログラム41aがコンピュータ40を制御することにより、各センタにおいて各エンティティ固有の秘密鍵を生成する。

【0074】

コンピュータ40の内部に設けられた記録媒体42は、内蔵設置される例えばハードディスクドライブまたはROMなどを用いてなり、記録媒体42には前述の如きプログラム42aが記録されている。記録媒体42から読み出されたプログラム42aがコンピュータ40を制御することにより、各センタにおいて各エンティティ固有の秘密鍵を生成する。

【0075】

コンピュータ40に設けられたディスクドライブ40aに装填して使用される記録媒体43は、運搬可能な例えば光磁気ディスク、CD-ROMまたはフレキ

シブルディスクなどを用いてなり、記録媒体 4 3 には前述の如きプログラム 4 3 a が記録されている。記録媒体 4 3 から読み出されたプログラム 4 3 a がコンピュータ 4 0 を制御することにより、各センタにおいて各エンティティ固有の秘密鍵を生成する。

【0 0 7 6】

【発明の効果】

本発明では、エンティティの各分割特定情報に応じて対称行列の一部の成分を取り出し、取り出した成分に各エンティティ固有の乱数を合成して、各エンティティ固有の秘密鍵を生成するようにしたので、個人乱数を加えることによってセンタの秘密が露呈されず、安全性を向上することができる。

【0 0 7 7】

また、自身で生成したハッシュ関数と他のセンタで生成されたハッシュ関数とを用いて、取り出した成分に合成すべき乱数を生成するようにしたので、全てのセンタが対等となり、ある特定のセンタがBig Brother となることを防止できる。

【0 0 7 8】

また、エンティティの各分割特定情報に応じて対称行列の一部の成分を取り出し、その分割特定情報に基づいて各センタ固有のマスクパターンを生成し、取り出した成分をそのマスクパターンでマスクして、各エンティティ固有の秘密鍵を生成するようにしたので、両エンティティにおいて分割特定情報が同じであっても、そのマスクパターンは異なるため、結託攻撃に強くなり、結託閾値を高くすることができる。

【0 0 7 9】

また、以上のような個人乱数付加とマスク処理とを融合させて各エンティティ固有の秘密鍵を生成するようにしたので、乱数置換攻撃を全く受けない暗号方式を提供できる。更に、本発明では、共通鍵を生成する際に各センタからの成分をXOR合成しており、桁上がりの問題を解消できる。

【0 0 8 0】

(付記)

なお、以上の説明に対して更に以下の項を開示する。

(1) 請求項 2 に記載の秘密鍵生成方法であって、 $J$  個のセンタが存在し、 $j$  番目 ( $j = 1, 2, \dots, J$ ) のセンタは自身が生成した前記ハッシュ関数を ( $j + 1$ ) 番目 ( $j = J$  の場合は 1 番目) のセンタへ送付し、( $j + 1$ ) 番目 ( $j = J$  の場合は 1 番目) のセンタにて、自身が生成したハッシュ関数と送付された  $j$  番目のセンタのハッシュ関数とに基づいて、自身での前記乱数を生成する秘密鍵生成方法。

(2) 複数のセンタの夫々にて、エンティティの特定情報を複数のブロックに分割した各分割特定情報と各センタ毎の秘密の対称行列とを用いて、前記エンティティ固有の秘密鍵を生成する方法において、前記各分割特定情報に応じて前記対称行列の一部の成分を取り出し、前記各分割特定情報に応じて各センタ固有のマスクパターンを生成し、取り出した成分を前記マスクパターンでマスクし、そのマスク結果に前記エンティティ固有の乱数を合成することにより、前記エンティティ固有の秘密鍵を生成する秘密鍵生成方法。

(3) 第 (2) 項に記載の秘密鍵生成方法であって、一のセンタ自身で生成したハッシュ関数と他のセンタで生成されたハッシュ関数とに基づいて、前記一のセンタでの前記乱数を生成する秘密鍵生成方法。

(4) 第 (3) 項に記載の秘密鍵生成方法であって、 $J$  個のセンタが存在し、 $j$  番目 ( $j = 1, 2, \dots, J$ ) のセンタは自身が生成した前記ハッシュ関数を ( $j + 1$ ) 番目 ( $j = J$  の場合は 1 番目) のセンタへ送付し、( $j + 1$ ) 番目 ( $j = J$  の場合は 1 番目) のセンタにて、自身が生成したハッシュ関数と送付された  $j$  番目のセンタのハッシュ関数とに基づいて、自身での前記乱数を生成する秘密鍵生成方法。

(5) 複数のセンタの夫々にて、各エンティティの特定情報を複数のブロックに分割した各分割特定情報と各センタ毎の秘密の対称行列とを用いて、各エンティティ固有の秘密鍵を生成し、この秘密鍵に含まれている暗号文の送信先である相手のエンティティに対応する成分を使用して生成した共通鍵を用いて平文を暗号文に暗号化する暗号化方法において、請求項 1 ~ 3, 第 (1) 項 ~ 第 (4) 項の何れかに記載の秘密鍵生成方法によって生成された各エンティティ固有の秘密



鍵を使用する暗号化方法。

(6) エンティティ間の暗号通信にあって、平文から暗号文への暗号化処理及び暗号文から平文への復号処理に用いる共通鍵を生成する方法において、一方のエンティティの特定情報を複数のブロックに分割した各分割特定情報を用いて生成された前記一方のエンティティ固有の各秘密鍵に含まれている通信相手の他方のエンティティに対応する成分を夫々取り出し、取り出した成分をXOR合成して前記共通鍵を生成する共通鍵生成方法。

(7) エンティティ間の暗号通信にあって、平文から暗号文への暗号化処理及び暗号文から平文への復号処理に用いる共通鍵を生成する方法において、請求項1～3、第(1)項～第(4)項の何れかに記載の秘密鍵生成方法によって生成された一方のエンティティ固有の各秘密鍵に含まれている通信相手の他方のエンティティに対応する成分を夫々取り出し、取り出した成分をXOR合成して前記共通鍵を生成する共通鍵生成方法。

(8) センタから各エンティティへ各エンティティ固有の秘密鍵を送付し、一方のエンティティが前記センタから送付された該エンティティ固有の秘密鍵から求めた共通鍵を用いて平文を暗号文に暗号化して他方のエンティティへ伝送し、該他方のエンティティが伝送された暗号文を、前記センタから送付された該エンティティ固有の秘密鍵から求めた、前記共通鍵と同一の共通鍵を用いて元の平文に復号することにより、エンティティ間で情報の通信を行うこととし、前記センタが複数設けられており、その複数のセンタ夫々は、各エンティティ固有の秘密鍵を生成するようにした暗号通信方法において、請求項1～3、第(1)項～第(4)項の何れかに記載の秘密鍵生成方法によって各エンティティ固有の秘密鍵を生成する暗号通信方法。

(9) センタから各エンティティへ各エンティティ固有の秘密鍵を送付し、一方のエンティティが前記センタから送付された該エンティティ固有の秘密鍵から求めた共通鍵を用いて平文を暗号文に暗号化して他方のエンティティへ伝送し、該他方のエンティティが伝送された暗号文を、前記センタから送付された該エンティティ固有の秘密鍵から求めた、前記共通鍵と同一の共通鍵を用いて元の平文に復号することにより、エンティティ間で情報の通信を行うこととし、前記セン

タが複数設けられており、その複数のセンタ夫々は、各エンティティ固有の秘密鍵を生成し、各エンティティは、自身固有の複数の秘密鍵に含まれている相手のエンティティに対応する成分を使用して前記共通鍵を生成するようにした暗号通信方法において、請求項1～3，第（1）項～第（4）項の何れかに記載の秘密鍵生成方法によって一方のエンティティ固有の秘密鍵を生成し、生成された一方のエンティティ固有の各秘密鍵に含まれている通信相手の他方のエンティティに対応する成分を夫々取り出し、取り出した成分をXOR合成して前記共通鍵を生成する暗号通信方法。

（10） 送信すべき情報である平文を暗号文に暗号化する暗号化处理、及び、送信された暗号文を元の平文に復号する復号処理を、複数のエンティティ間で相互に行うこととし、各エンティティ固有の秘密鍵を生成して各エンティティへ送付する複数のセンタと、該センタから送付された自身固有の複数の秘密鍵に含まれている通信対象のエンティティに対応する成分を使用して、前記暗号化处理及び復号処理に用いる共通鍵を生成する複数のエンティティとを有する暗号通信システムにおいて、請求項1～3，第（1）項～第（4）項の何れかに記載の秘密鍵生成方法によって各エンティティ固有の秘密鍵を生成するようにした暗号通信システム。

（11） コンピュータに、エンティティの特定情報を複数のブロックに分割した各分割特定情報と秘密の対称行列とを用いて、前記エンティティ固有の秘密鍵を生成させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体において、前記各分割特定情報に応じて前記対称行列の一部の成分を取り出すことをコンピュータに実行させるプログラムコード手段と、取り出した成分に前記エンティティ固有の乱数を合成することにより、前記エンティティ固有の秘密鍵を生成することをコンピュータに実行させるプログラムコード手段とを含むプログラムが記録されている記録媒体。

（12） コンピュータに、エンティティの特定情報を複数のブロックに分割した各分割特定情報と秘密の対称行列とを用いて、前記エンティティ固有の秘密鍵を生成させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体において、前記各分割特定情報に応じて前記対称行列の一部の成分

を取り出すことをコンピュータに実行させるプログラムコード手段と、前記各分割特定情報に応じてマスクパターンを生成することをコンピュータに実行させるプログラムコード手段と、取り出した成分を前記マスクパターンでマスクすることにより、前記エンティティ固有の秘密鍵を生成することをコンピュータに実行させるプログラムコード手段とを含むプログラムが記録されている記録媒体。

【図面の簡単な説明】

【図 1】

本発明の暗号通信システムの構成を示す模式図である。

【図 2】

2 人のエンティティ間における情報の通信状態を示す模式図である。

【図 3】

エンティティの I D ベクトルの分割例を示す模式図である。

【図 4】

記録媒体の実施の形態の構成を示す図である。

【図 5】

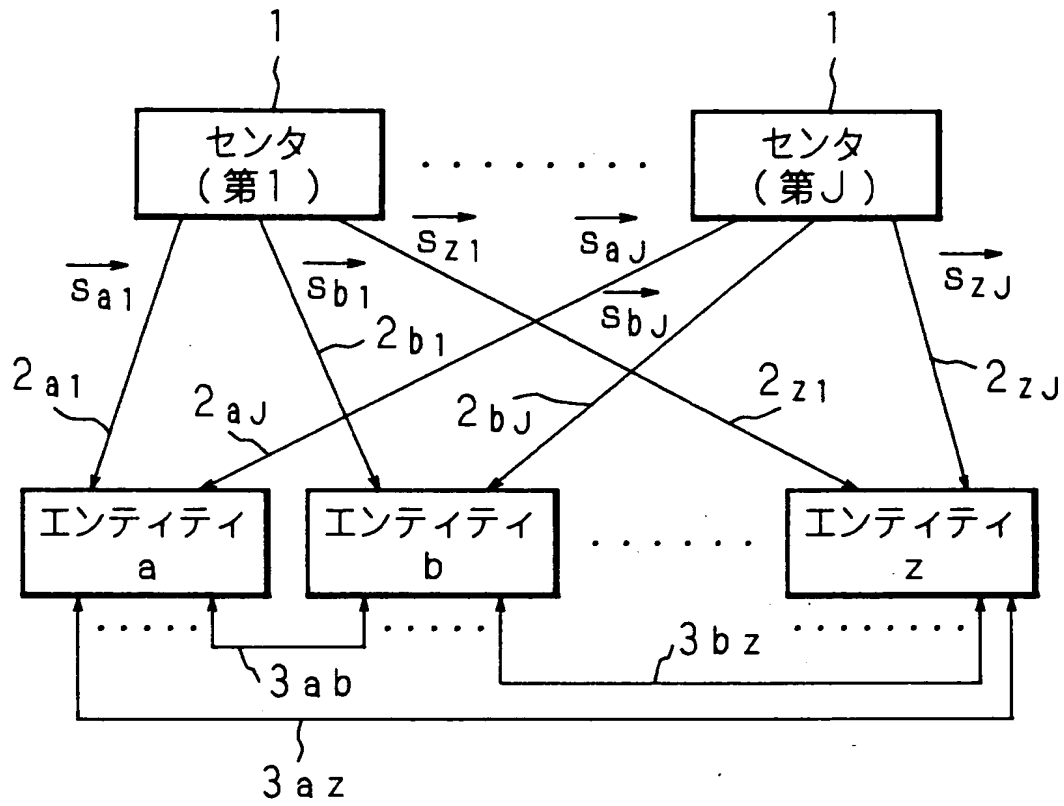
I D - N I K S のシステムの原理構成図である。

【符号の説明】

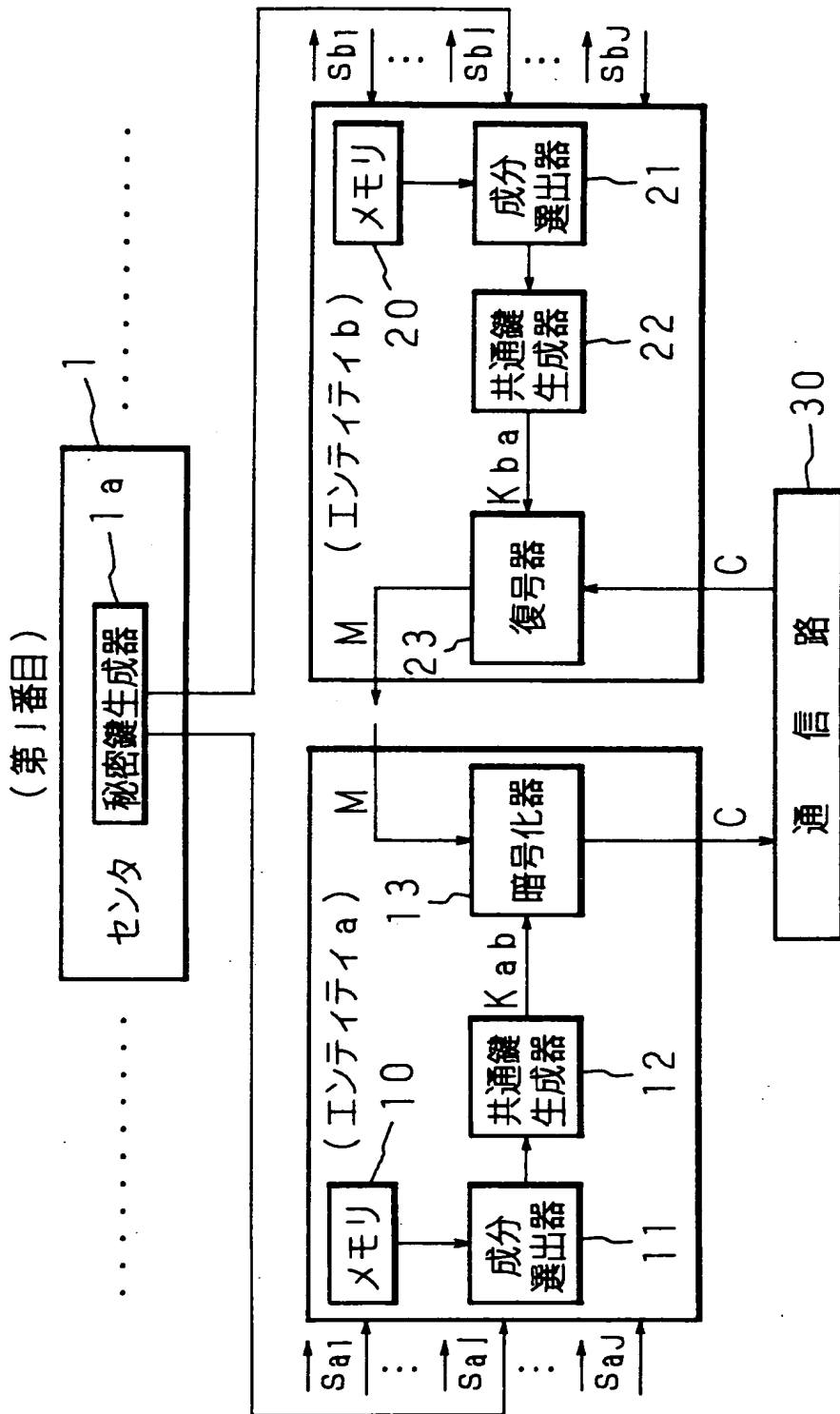
- 1 センタ
- 1 a 秘密鍵生成器
- 1 0, 2 0 メモリ
- 1 1, 2 1 成分選出器
- 1 2, 2 2 共通鍵生成器
- 1 3 暗号化器
- 2 3 復号器
- 3 0 通信路
- 4 0 コンピュータ
- 4 1, 4 2, 4 3 記録媒体

【書類名】 図面

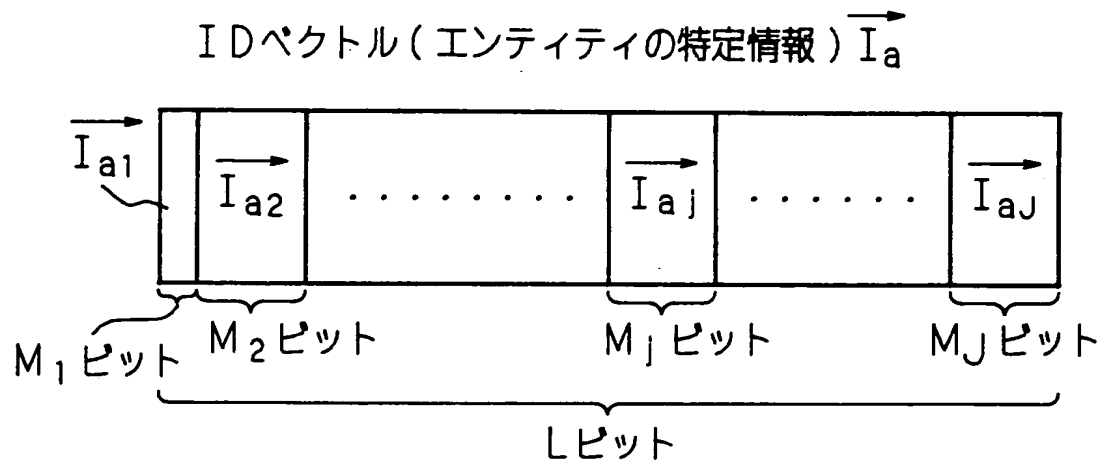
【図 1】



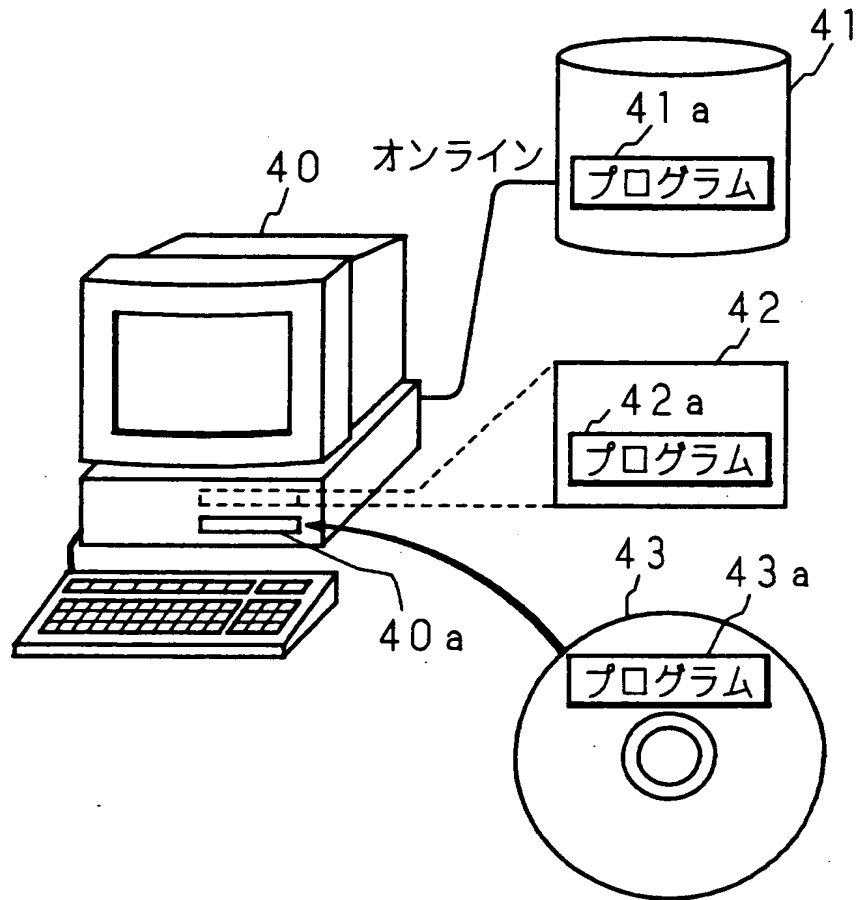
【図 2】



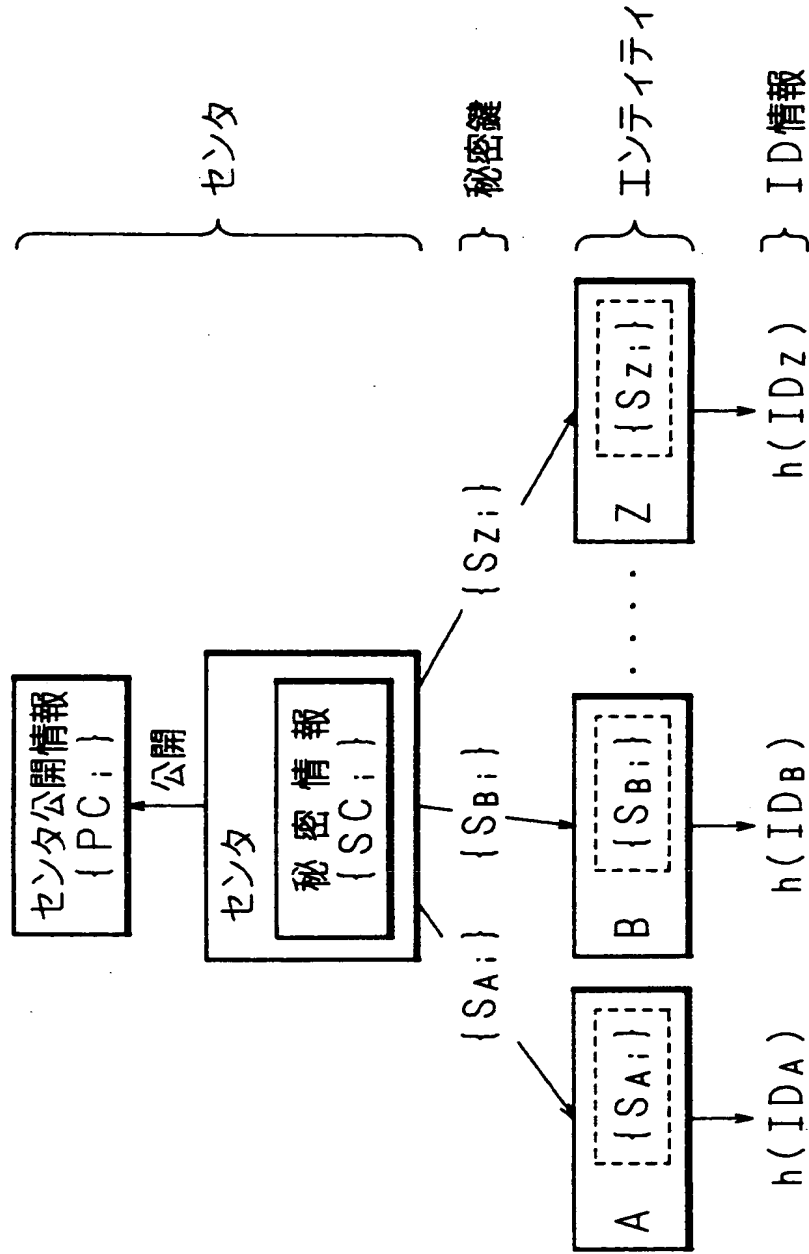
【図 3】



【図4】



【図 5】





【書類名】            要約書

【要約】

【課題】    エンティティ間で高速に鍵共有を行え、しかも安全性が高い I D - N I K S による暗号通信システムを提供する。

【解決手段】    各エンティティの特定情報を複数のブロックに分割した各分割特定情報と各センタ 1 毎の秘密の対称行列とを用いて、各エンティティ固有の秘密鍵を生成する際に、各分割特定情報に応じてその対称行列の一部の成分を取り出し、取り出した成分に各エンティティ固有の乱数を合成して、各エンティティ固有の秘密鍵を生成する。

【選択図】            図 1

認定・付加情報

特許出願の番号	特願 2000-016354
受付番号	50000073733
書類名	特許願
担当官	坪 政光 8844
作成日	平成12年 5月22日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000006297
【住所又は居所】	京都府京都市南区吉祥院南落合町3番地
【氏名又は名称】	村田機械株式会社

【特許出願人】

【識別番号】	597008636
【住所又は居所】	大阪府箕面市粟生外院4丁目15番3号
【氏名又は名称】	笠原 正雄

【特許出願人】

【識別番号】	598159964
【住所又は居所】	東京都渋谷区神宮前四丁目2番19号
【氏名又は名称】	辻井 重男

【復代理人】

【識別番号】	100114557
【住所又は居所】	大阪府大阪市中央区釣鐘町二丁目4番3号 河野 特許事務所
【氏名又は名称】	河野 英仁

【代理人】

申請人	
【識別番号】	100078868
【住所又は居所】	大阪府大阪市中央区釣鐘町二丁目4番3号 河野 特許事務所
【氏名又は名称】	河野 登夫

出 願 人 履 歴 情 報

識別番号 [000006297]

1. 変更年月日 1990年 8月 7日  
[変更理由] 新規登録  
住 所 京都府京都市南区吉祥院南落合町3番地  
氏 名 村田機械株式会社

出 願 人 履 歴 情 報

識別番号 [ 5 9 7 0 0 8 6 3 6 ]

1. 変更年月日 1 9 9 7 年 1 月 2 1 日

[変更理由] 新規登録

住 所 大阪府箕面市栗生外院4丁目15番3号

氏 名 笠原 正雄

出 願 人 履 歴 情 報

識別番号 [598159964]

1. 変更年月日	1998年11月19日
[変更理由]	新規登録
住 所	東京都渋谷区神宮前四丁目2番19号
氏 名	辻井 重男